Infrastruktura më qelës publik

Kriptografia me qelës publik

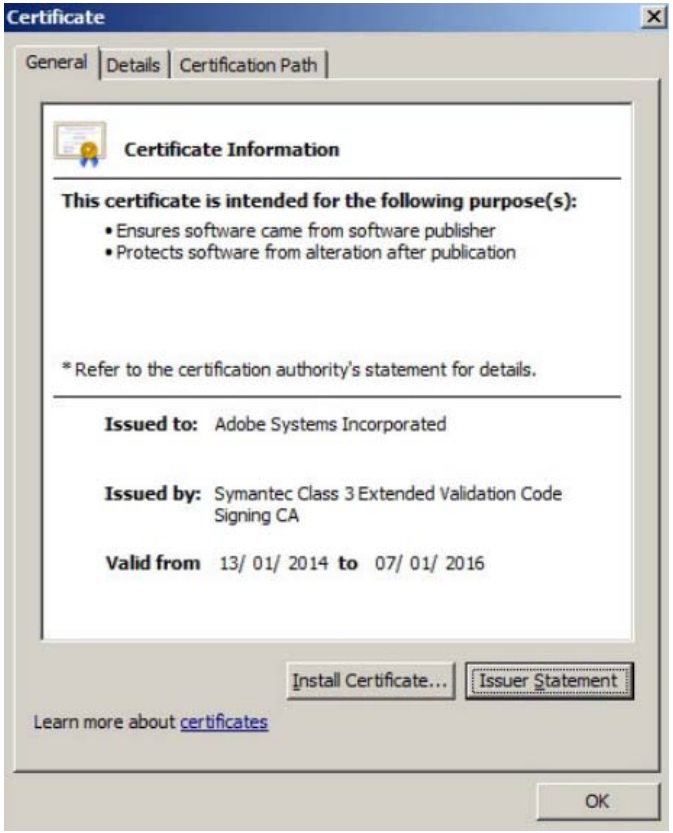
Përdorimi i Nënshkrimit Digjital

- Nënshkrimet digjitale janë një teknikë matematikore e përdorur për të siguruar autenticitetin, integritetin dhe mosnjohjen në formën e nënshkrimit të kodeve dhe certifikatave dixhitale.
  - Nënshkrimet digjitale zakonisht përdoren në dy situatat e mëposhtme:
  - Nënshkrimi i kodeve - nënshkrimi i kodit përdoret për të verifikuar integritetin e skedarëve ekzekutues të shkarkuar nga një uebsajt shitësish.
- Certifikatat digjitale - Këto përdoren për të vërtetuar identitetin e një sistemi dhe për të shkëmbyer të dhëna konfidenciale.
  - Ekzistojnë tre algoritme të Standardeve të Nënshkrimit Digital (DSS) të përdorura për gjenerimin dhe verifikimin e nënshkrimit digjital:
  - Algoritmi i Nënshkrimit Digital (DSA)
  - Rivest-Shamir Adelman Algoritmi (RSA)
  - Algoritmi i nënshkrimit të algjeve eliptike (ECDSA)

Kriptografia me qelës publik

Nënshkrimet Digjitale për kodim

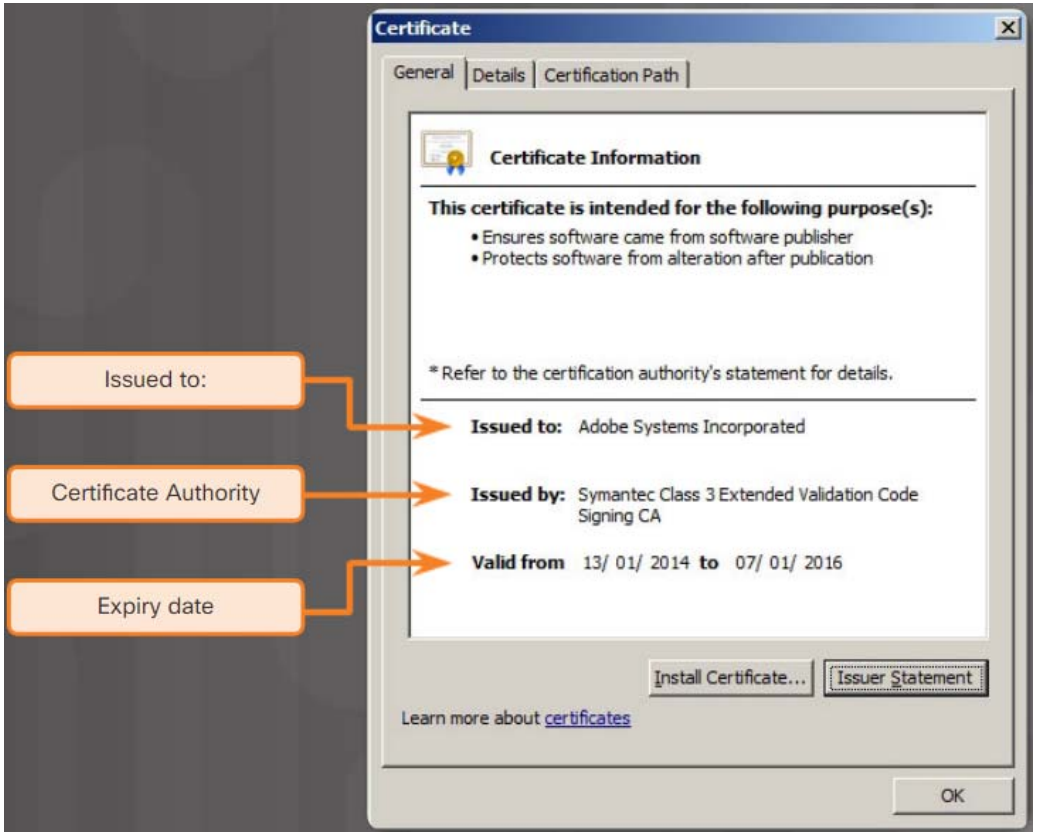
- Nënshkrimet digjitale zakonisht përdoren për të siguruar siguri për origjinalitetin dhe integritetin e kodit të softuerit.
- Dosjet e ekzekutueshme janë të mbështjellura në një zarf të nënshkruar në mënyrë digjitale, gjë që i lejon përdoruesit përfundimtar të verifikojë nënshkrimin para instalimit të softuerit.
- Kodi i nënshkrimit digjital siguron disa siguri rreth kodit:
  - Kodi është autentik dhe në fakt vjen nga botuesi.
  - Kodi nuk është modifikuar pasi që u largua nga botuesi i softuerit.
  - Botuesi publikoi në mënyrë të pamohueshme kodin. Kjo siguron mosnjohje të aktit të botimit.



Kriptografia me qelës publik

Nënshkrimet Digjitale per Certifikata Digjitale

- Një certifikatë dixhitale u mundëson përdoruesve, pretëve dhe organizatave të shkëmbejnë informacione të sigurta nëpërmjet internetit.
- Në mënyrë të veçantë, një certifikatë dixhitale përdoret për të vërtetuar dhe verifikuar që përdoruesit që dërgojnë një mesazh janë ata që pretendojnë të jenë.
- Certifikatat digjitale mund të përdoren gjithashtu për të siguruar konfidencialitet për pranuesin me mjetet për të koduar një përgjigje.

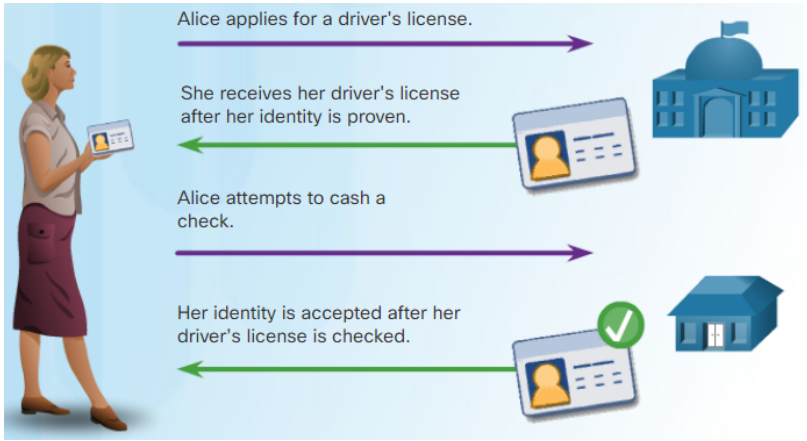


Autoritetet dhe Sistemit I Besimit PKI

Menaxhimi I Qelësit Publik

- Kur vendoset një lidhje asimetrike midis dy ushtrive, pret do të shkëmbejnë informatat e tyre kryesore publike.
- Palët e treta të besuara në internet vërtetojnë vërtetësinë e këtyre çelësave publikë duke përdorur certifikatat digjitale. Pala e tretë lëshon kredencialet që janë vështirë të krijohen.
- Prej asaj pike përpara, të gjithë individët që i besojnë palës së tretë thjesht pranojnë kredencialet që lëshon pala e tretë.

- Infrastruktura me qeles publike (PKI) është një shembull i një sistemi të besuar të palëve të treta të referuara si autoritet certifikimi (CA).
- AK lëshon certifikata digjitale që vërtetojnë identitetin e organizatave dhe përdoruesve.
- Këto certifikata përdoren gjithashtu për të nënshkruar mesazhe për të siguruar që mesazhet të mos jenë të manipuluara.



Autoritetet dhe Sistemit I Besimit PKI

Infrastruktura e Qelësit Publik

- PKI është e nevojshme për të mbështetur shpërndarjen në shkallë të gjerë dhe identifikimin e çelësave të enkriptimit publik.
- Korniza PKI lehtëson një marrëdhënie shumë të shkallëzuar të besimit.
- Përbëhet nga hardueri, softueri, njerëzit, politikat dhe procedurat e nevojshme për krijimin, menaxhimin, ruajtjen, shpërndarjen dhe revokimin e certifikatave digjitale.
- Jo të gjitha certifikatat e PKI pranohen direkt nga një AK. Një autoritet regjistrimi (RA) është një autorizim i varur dhe është i certifikuar nga një CA rrënjë për të lëshuar certifikata për përdorime specifike.

Autoritetet dhe Sistemit I Besimit PKI

Sistemi I Autoriteteve të PKI

- Shitësit Shumë ofrojnë servera CA si një shërbim i menaxhuar ose si një produkt i përdoruesit të fundit.
- Organizatat gjithashtu mund të zbatojnë PKI-të private duke përdorur Microsoft Server ose Open SSL.
- CA lëshon certifikata bazuar në klasa që përcaktojnë se sa besohet një certifikatë.
- Numri i klasës përcaktohet nga mënyra rigoroze e procedurës që ka vërtetuar identitetin e mbajtësit kur është lëshuar certifikata.
- Sa më i lartë numri i klasës, aq më i besuar është certifikata.
- Disa çelësa publikë të CA-së janë të parapërgatitur, të tilla si ato të listuara në shfletuesit e uebit.
- Një ndërmarrje gjithashtu mund të zbatojë PKI për përdorim të brendshëm.

Class	Description
0	Used for testing purposes in which no checks have been performed.
1	Used for individuals with a focus on verification of email.
2	Used for organizations for which proof of identity is required.
3	Used for servers and software signing for which independent verification and checking of identity and authority is done by the issuing certificate authority.
4	Used for online business transactions between companies.
5	Used for private organizations or governmental security.

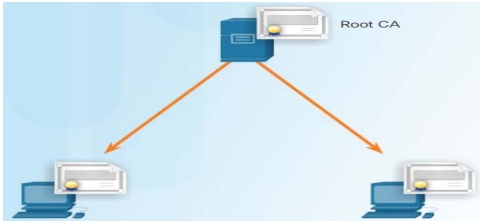
Autoritetet dhe Sistemit I Besimit PKI

Sistemi I Besimit të PKI

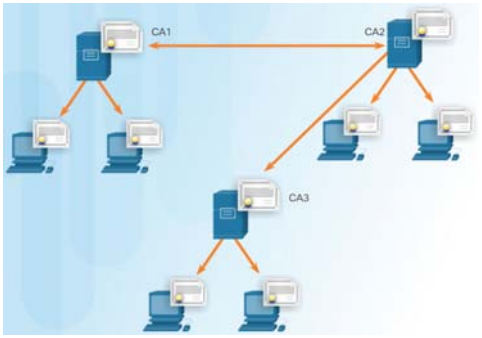
- PKI-të mund të formojnë topologji të ndryshme të besimit. Më e thjeshtë është topologjia PKI me rrënjë të vetme.

Në rrjetet më të mëdha, CA-të e PKI mund të lidhen duke përdorur dy arkitektura bazë:

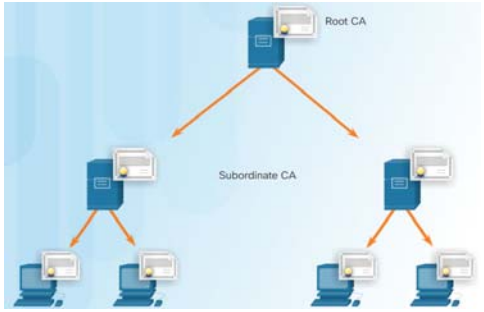
- Topologji CA të kryqëzuara - Ky është një model peer-to-peer në të cilin CA-të individuale krijojnë marrëdhënie besimi me CA të tjera duke certifikuar vërtetimin e CA-së.
- Topologji hierarkike të CA-së - Niveli më i lartë CA quhet rrjeti CA. Ajo mund të lëshojë certifikata për përdoruesit përfundimtarë dhe për një CA vartës.



Single-Root PKI



Cross-certified CA

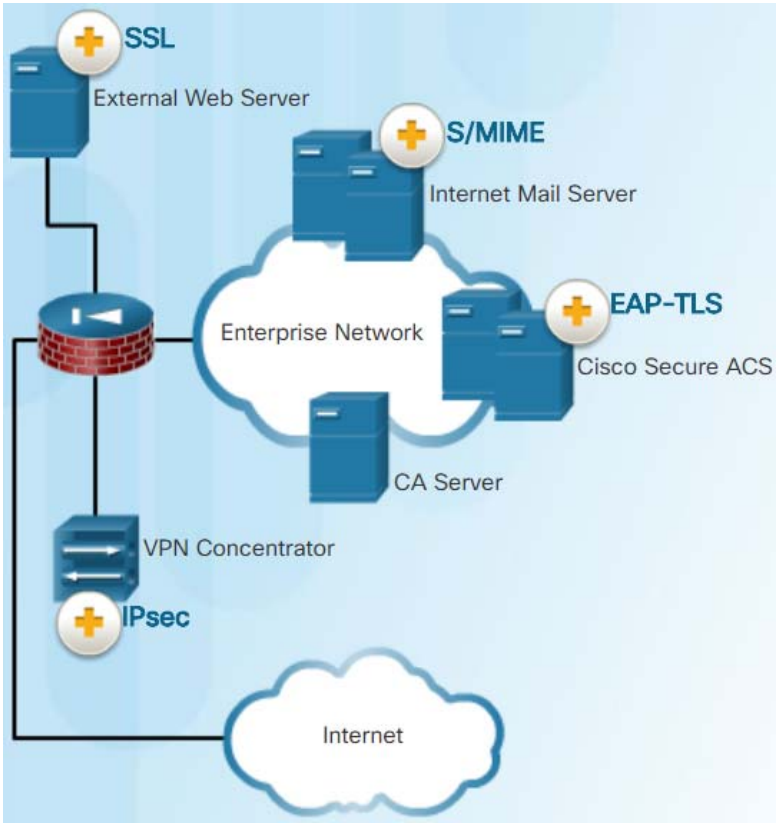


Hierarchical CA

Autoritetet dhe Sistemit I Besimit PKI

Ndërveprimi i shitësve të ndryshëm të PKI

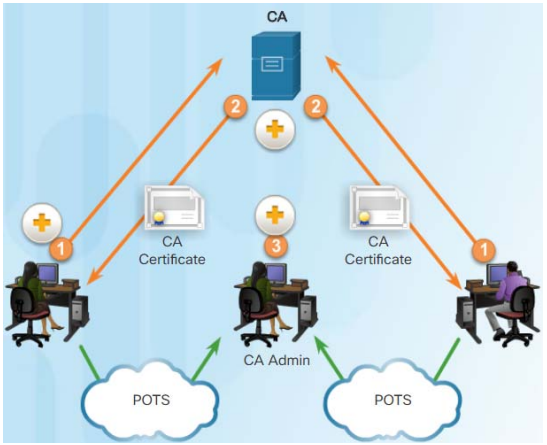
- Ndërveprimi midis një PKI dhe shërbimeve mbështetëse të tij është një shqetësim, sepse shumë shitës të CA kanë propozuar dhe zbatuar zgjidhje pronësore në vend që të presin që standardet të zhvillohen.
- Për të trajtuar këtë shqetësim të ndërveprimit, IETF publikoi Internetin X.509 Politikat Publike të Çertifikimit të Infrastrukturës dhe Kornizën e Praktikave të Certifikimit (RFC 2527).
- Standardi X.509 version 3 (X.509v3) përcakton formatin e një certifikate dixhitale.



Autoritetet dhe Sistemi i Besimit PKI

Regjistrimi i Certifikatave, Autentifikimi dhe Revokimi

- Të gjitha sistemet që përdorin PKI duhet të kenë çelësin publik të AK-së, të quajtur certifikata e vetë-nënshkruar.
- Çelësi publik i AK-së verifikon të gjitha certifikatat e lëshuara nga AK dhe është jetike për funksionimin e duhur të PKI.
- Procesi i rregjistrimit të certifikatës fillon kur certifikatat e CA-së shfridhen në brez përgjatë një rrjeti dhe autentifikimi bëhet me anë të telefonit (OOB).
- Sistemi që regjistrohet me PKI kontakton një AK për të kërkuar dhe për të marrë një çertifikatë dixhitale identiteti për vete dhe për të marrë certifikatën e vetëshkruar të Autoritetit Kontraktues.
- Faza përfundimtare verifikon që certifikata e Autoritetit Kontraktues është autentik dhe kryhet duke përdorur një metodë OOB si sistemi i thjeshtë i telefonave të vjetër (POTS) për të marrë shenjën e gishtit të certifikatës së identitetit të vlefshëm të CA.
- Një çertifikatë dixhitale mund të revokohet nëse kyç është kompromet uar ose nëse nuk është më i nevojshëm.



Aplikimet dhe Ndikimet e Kriptografisë

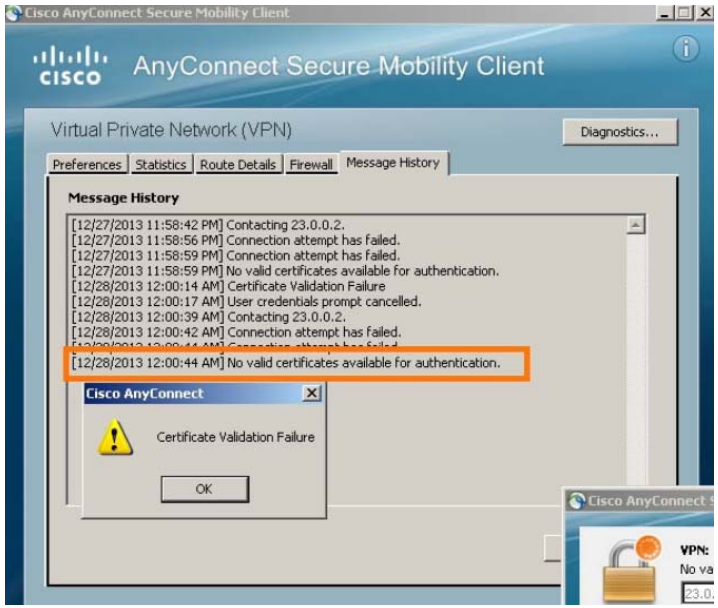
Aplikimi i PKI

- Disa nga aplikimet e shumta të PKI-ve janë:
  - SSL / TLS çertifikatë me bazë peer authentication
  - Trafiku i sigurt i rrjetit duke përdorur IPsec VPN
  - Trafiku Web HTTPS
  - Kontrollo qasjen në rrjet duke përdorur 802.1x authentication
  - Sigurohuni me email duke përdorur protokollin S / MIME
  - Mesazhe të menjëhershme të sigurta
  - Miraton dhe autorizon aplikimet me nënshkrimin e kodit
  - Mbroni të dhënat e përdoruesit me Sistemin e Dhënave të Encryption (EFS)
  - Zbatimi i legalizimit me dy faktorë me karta inteligjente
  - Sigurimi i pajisjeve ruajtëse USB

Aplikimet dhe Ndikimet e Kriptografisë

Kriptimi i transaksioneve në rrjet

- Akterët e kërcënimit mund të përdorin SSL / TLS për të futur shkeljet e pajtueshmërisë rregullatore, viruset, malware, humbjet e të dhënave dhe përpjekjet e ndërhyrjes në një rrjet.
- Çështje të tjera të lidhura me SSL / TLS mund të lidhen me vërtetimin e certifikatës së një web server. Kur kjo ndodh, shfletuesit e internetit do të shfaqin një paralajmërim për sigurinë. Çështjet që lidhen me PKI që lidhen me paralajmërimet e sigurisë përfshijnë:
  - Afati i datës së vlefshmërisë - Certifikatat X.509v3 specifikojnë datat "jo para" dhe "nuk pas". Nëse data e tanishme është jashtë intervalit, shfletuesi web shfaq një mesazh.
  - Gabimi i vërtetimit të nënshkrimit - Nëse një shfletues nuk mund ta vërtetojë nënshkrimin në çertifikatë, nuk ka siguri se çelësi publik i certifikatës është autentik.



Aplikimet dhe Ndikimet e Kriptografisë

Enkriptimi dhe monitorimi i sigurisë

- Monitorimi i rrjetit bëhet më sfidues kur paketat janë të koduara.
- Për shkak se HTTPS paraqet trafikun HTTP të koduar nga fundi në fund (përmes TLS / SSL), nuk është aq e lehtë të shikosh trafikun e përdoruesit.
- Këtu është një listë e disa prej gjërave që një analist i sigurisë mund të bënte:
  - Konfiguro rregullat për të dalluar trafikun SSL dhe jo SSL, HTTPS dhe trafikun SSL jo-HTTPS.
  - Rritja e sigurisë përmes validimit të certifikatës së serverit duke përdorur CRLs dhe OCSP.
  - Zbatimi i mbrojtjes së antimalware dhe filtrimi URL i përmbajtjes së HTTPS.
  - Vendosni një Cisco SSL Appliance për të dekriptuar trafikun SSL dhe për ta dërguar atë në aparatet e sistemit të parandalimit të ndërhyrjeve (IPS) për të identifikuar rreziqet e fshehura normalisht nga SSL.

Përmbledhje

- Sigurimi i komunikimit me kriptografi përbëhet nga katër elemente:
  - Konfidencialiteti i të dhënave për të garantuar që vetëm përdoruesit e autorizuar mund ta lexojnë mesazhin.
  - Integriteti i të dhënave për të garantuar që mesazhi nuk është ndryshuar.
  - Authentication origjinës garanton se mesazhi nuk është një falsifikim dhe në fakt vjen nga kush thuhet.
  - Mosdeklarimi i të dhënave për të garantuar që dërguesi nuk mund të refuzojë ose të refuzojë vlefshmërinë e një mesazhi të dërguar.
- Cryptology është shkenca e bërjes dhe thyerjes së kodeve sekrete. Ekzistojnë dy disiplina: kriptografi dhe kriptanaliza.
- Një shifër është një algoritëm që përbëhet nga një seri hapash të përcaktuar mirë që mund të ndiqen si një procedurë kur kriptimi dhe dekriptimi i mesazheve.
- Ekzistojnë një numër i metodave të thyerjes së kodit (cryptanalysis), të tilla si forca brutale, ciphertext dhe i njohur tekst-plaintext, ndër të tjera.
- Me teknologjinë moderne, siguria e enkriptimit qëndron në sekretin e çelësave, jo në algoritmin. Në mënyrë të veçantë gjatësia kryesore dhe hapësira e çelësave.

Përmbledhje

- Hierat kriptografike përdoren për të verifikuar dhe siguruar integritetin e të dhënave.
- Funksionet Hash e bëjnë atë të pakalueshme për dy grupe të ndryshme të të dhënave për të dalë me të njëjtin output hash.
- Matematikisht, ekuacioni h = H (x) përdoret për të shpjeguar se si funksionon një algoritëm hash.
- Tre funksione të njohura hash përfshijnë:
  - MD5 me një digest 128-bit
  - SHA-1
  - SHA-2
- Për të përfshirë vërtetimin së bashku me integritetin e mesazhit, një HMAC shtohet si një hyrje për një funksion hash. Nëse dy palët ndajnë një çelës sekret dhe përdorin funksionet e HMAC për autentikim, një trillim HMAC i ndërtuar siç duhet i një mesazhi që një parti ka marrë tregon se pala tjetër ishte autori i mesazhit.
- Konfidencialiteti i të dhënave sigurohet nëpërmjet një prej dy llojeve të encryption: simetrike dhe asimetrike.

Përmbledhje

- Konfidencialiteti i të dhënave sigurohet nëpërmjet një prej dy llojeve të encryption: simetrike dhe asimetrike.
- Algoritmet simetrike përdorin të njëjtin çelës të parazgjedhur për të koduar dhe dekriptuar të dhënat.
- Algoritmet simetrike të enkriptimit klasifikohen shpesh si: Shifrat e bllokut ose Shifrat e rrymës.
- Algoritmet asimetrike, të quajtura edhe algoritme me çelës publik, janë projektuar në mënyrë që çelësi që përdoret për encryption është i ndryshëm nga çelësi që përdoret për decryption.
- Algoritmet asimetrike përdoren për të siguruar konfidencialitet pa para-ndarjen e një fjalëkalimi. Qëllimi i konfidencialitetit të algoritmeve asimetrike fillohet kur procesi i enkriptimit fillon me çelësin publik.
- Qëllimi i legalizimit të algoritmave asimetrike është iniciuar me procesin e enkriptimit të çelësit privat. Përdorni formulën: Çelësi Privat (Encrypt) + Çelësi Publik (Dekripto) = Autentifikim.
- Kombinimi i dy proceseve të encryption asimetrike siguron konfidencialitetin, autentifikimin dhe integritetin e mesazhit.
- Diffie-Hellman (DH) është një algoritëm matematik asimetrik që lejon dy kompjuterë të gjenerojnë një sekret identik të përbashkët pa u komunikuar më parë.

Përmbledhje

- Nënshkrimet digjitale janë një teknikë matematikore e përdorur për të siguruar origjinalitetin, integritetin dhe mosnjohjen në formën e nënshkrimit të kodeve dhe certifikatave digjitale.
- Nënshkrimet digjitale zakonisht përdoren për të siguruar siguri për origjinalitetin dhe integritetin e kodit të softuerit.
- Një certifikatë dixhitale u mundëson përdoruesve, pretëve dhe organizatave të shkëmbejnë informacione të sigurta nëpërmjet internetit.
- Infrastruktura kryesore publike (PKI) është një shembull i një sistemi të besuar të palëve të treta të referuara si autoritet certifikimi (CA).
- PKI është e nevojshme për të mbështetur shpërndarjen në shkallë të gjerë dhe identifikimin e çelësave të enkriptimit publik.
- Shitësit e shumtë ofrojnë shërbime CA si një shërbim i menaxhuar ose si një produkt i përdoruesit të fundit. Organizatat gjithashtu mund të zbatojnë PKI private duke përdorur Microsoft Server ose Open SSL. CA lëshon certifikata bazuar në klasa që përcaktojnë se sa besohet një certifikatë.
- PKI-të mund të formojnë topologji të ndryshme të besimit. Më e thjeshtë është topologjia PKI me një rrënjë. Në rrjetet më të mëdha, CA-të e PKI-së mund të lidhen duke përdorur dy arkitektura bazë: Topologji CA të kryqëzuara dhe topologji Hierarkike CA.

Përmbledhje

- Ndërveprimi midis një PKI dhe shërbimeve mbështetëse të tij është një shqetësim, sepse shumë shitës të CA kanë propozuar dhe zbatuar zgjidhje pronësore në vend që të presin që standardet të zhvillohen. Për të trajtuar këtë shqetësim të ndërveprimit, IETF publikoi Internetin X.509 Politikat Publike të Çertifikimit të Infrastrukturës dhe Kornizën e Praktikave të Certifikimit (RFC 2527). Standardi X.509 version 3 (X.509v3) përcakton formatin e një certifikate dixhitale.
- Të gjitha sistemet që përdorin PKI duhet të kenë çelësin publik të AK-së, të quajtur certifikata e vetë-nënshkruar. Çelësi publik i AK-së verifikon të gjitha certifikatat e lëshuara nga AK dhe është jetike për funksionimin e duhur të PKI.
- Ka shumë aplikime të PKIs.
- Akterët e kërcënimit mund të përdorin SSL / TLS për të futur shkeljet e pajtueshmërisë rregullatore, viruset, malware, humbjet e të dhënave dhe përpjekjet e ndërhyrjes në një rrjet.
- Monitorimi i rrjetit bëhet më sfidues kur paketat janë të koduara. Për shkak se HTTPS prezanton trafikun HTTP të koduar nga fundi në fund (përmes TLS / SSL), nuk është aq e lehtë të shikosh trafikun e përdoruesit. Këtu është një listë e disa prej gjërave që një analist i sigurisë mund të bënte:
  - Konfiguro rregullat për të dalluar trafikun SSL dhe jo SSL, HTTPS dhe trafikun SSL jo-HTTPS.
  - Rritja e sigurisë përmes validimit të certifikatës së serverit duke përdorur CRLs dhe OCSP.
  - Zbatimi i mbrojtjes së antimalware dhe filtrimi URL i përmbajtjes së HTTPS.
  - Vendosni një Cisco SSL Appliance për të dekriptuar trafikun SSL dhe për ta dërguar atë në aparatet e sistemit të parandalimit të ndërhyrjeve (IPS) për të identifikuar rreziqet e fshehura normalisht nga SSL.